LEARNING MADE EASY

Okta Special Edition

Identity as a Service (IDaaS)

for dummies®
A Wiley Brand

Understand Identity as a Service (IDaaS)

Address security challenges and use cases

Adopt modern identity

Brought to you by

okta

Lawrence C. Miller

Frederico Hakamine

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. More than 7,950 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, visit **www.okta.com** or follow Okta on **www.okta.com/blog**.

Identity as a Service (IDaaS)

Okta Special Edition

by Lawrence C. Miller and Frederico Hakamine

for dummies®
A Wiley Brand

Identity as a Service (IDaaS) For Dummies®, Okta Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-70867-4 (pbk); ISBN 978-1-119-70866-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Associate Publisher: Katie Mohr

Business Development Representative:
Frazer Hossack, Karen Hattan

Production Editor:
Mohammed Zafar Ali

Table of Contents

Introduction

As a business expands and scales, it adapts with applications to streamline its network and operations. Where an employee may have once had one login and password, IT now manages hundreds of credentials for on-premises and Software as a Service (SaaS) apps, running on different platforms and multiple devices.

Likewise, many businesses now offer online products and services that require their customers to log in to a secure account. Thus, IT must now manage millions of credentials for the business's customers globally.

On top of all this, users are one of the major targets of attacks, with 81 percent of data breaches caused by weak or stolen credentials according to a recent Verizon "Data Breach Investigations Report (DBIR)." To mitigate these threats, organizations must rely on different ways of authenticating a user identity — beyond passwords.

Knowing one security slip-up can be the end of a business, identity and access management (IAM) solutions give IT the ability to bolster security and manage identity and access with the same speed and confidence for ten employees as for hundreds of thousands, and as easily for tens of thousands of customers as for hundreds of millions of customers. This capability protects user credentials and sensitive data, and frees employees from time-consuming manual tasks — like password resets and account provisioning — allowing them to focus on more challenging and value-added projects that drive company growth and profitability.

To leverage IAM services and security at scale, most organizations are adopting modern identity from the cloud — Identity as a Service (IDaaS). IDaaS provides robust and scalable identity, so organizations can manage user and customer access to its applications and services from anywhere in the world on any device. In this book, you'll learn what modern identity is all about and how IDaaS can help your enterprise.

About This Book

This book consists of five chapters that explore:

- The importance of identity, what it is, and how it has evolved (Chapter 1)
- What modern identity (Identity as a Service) is and how it helps organizations address identity challenges and different use cases (Chapter 2)
- The components of a modern identity solution (Chapter 3)
- New trends and innovations to address the future of identity (Chapter 4)
- Capabilities and benefits of modern identity (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead.

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — and we sure hope you'll appreciate these useful nuggets of information.

IN THIS CHAPTER

- Covering the basics of identity and why it's important
- Learning about the different domains of identity
- Tracing the history of identity services

Chapter 1
What Is Identity?

In this chapter, you explore what identity is all about and why it's important, the different domains of identity management, and how identity has evolved.

Understanding Identity and Why It Matters

Information technology has always been a precious resource and has therefore always required some sort of control over who has access to what.

Early local area networks (LANs) were originally built to share files and printers within an organization — but the really critical files and expensive color laser printers were only shared with the executives and marketing! The IT department needed to be able to identify the executives and marketing folks, so they could ensure that no one else in the company would see the sales projections or could print really cool graphics.

Going back even earlier, access to mainframe computers (circa the 1960s) was restricted to a handful of people within an organization. Of course, a locked room was usually all that was required to control access to the mainframe and identity was easy — if you didn't have horn-rimmed glasses and a pocket protector, you didn't get access.

Thus, identity and IT have always walked together (see Figure 1-1).

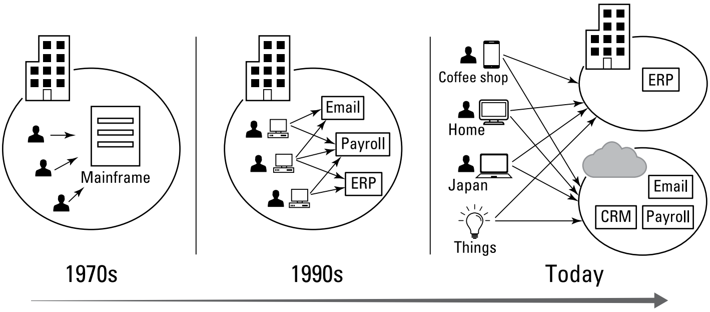

FIGURE 1-1: Identity and IT have always walked together. As IT evolves, the need for securely connecting people and things to technology increases.

Every time IT evolves, the need for identity and security evolves along with it. For example, in the 1990s and early 2000s, an organization's employees worked in office buildings. Their information was protected by a firewall installed at the perimeter between the corporate network and the Internet. Employees started their day by driving to the office, punching their time cards, and logging in from their desktop computers. At the end of the day, they logged off from their desktop computers and went home to their personal lives.

Then people got iPhones and laptops, and started working and collaborating more dynamically. Employees today read work emails on their personal smartphones, chat with friends, and send links across social media from their work laptops connected to open Wi-Fi networks in coffee shops, airports, and hotel lobbies. Today's reality — in which peoples' personal and work lives are increasingly co-mingled — is far removed from the well-defined and well-controlled workplace environment and network perimeter of the past.

Because people consume and interact with IT from any device and any place, security is no longer as simple as locking everyone into the office on a specific workstation and inherently trusting anyone inside the network perimeter. Organizations must be able to secure access to apps for any user while enforcing security on different network, system, and data contexts. They must also be able to manage those identities at scale, across a large ecosystem of employees and customers, on a multitude of systems located anywhere in the world. As IT continues to evolve, identity will always be there to keep you safe.

REMEMBER

Whenever you have shared resources or confidential information, you need identity to securely identify the individual using that resource or seeing that information. This allows you to limit what an individual can do (for example, who can use the color laser printer) or prevent others from seeing data or doing things that would harm an individual (for example, fraudulently seeing your Social Security number on your e-file tax return or buying stuff on Amazon with someone's credit card).

Identifying the Three Domains of Identity

Identity consists of the technologies that are used to solve three problems:

- Assert and verify an identity
- Determine what an identity can access and do
- Define the policies and processes used to manage identities within an organization's networks and systems

These technologies fall into three domains, shown in Figure 1-2 and described in the next three sections.

Identity and access management (IAM)

Broadly speaking, identity and access management, or IAM, is technology used to classify users and groups in a software system, as well as what resources they can access and what functions they can perform. IAM addresses authentication, authorization, account management, and access control.

IAM helps companies control who the users of its business are (that's the identity component) and what services they can or cannot access and how (that's the access management component).

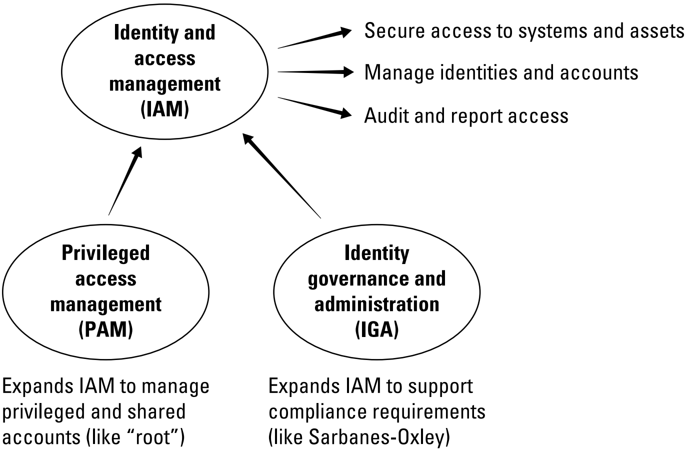
Identity and access management (IAM)
Secure access to systems and assets
Manage identities and accounts
Audit and report access
Privileged access management (PAM)
Identity governance and administration (IGA)
Expands IAM to manage privileged and shared accounts (like "root")
Expands IAM to support compliance requirements (like Sarbanes-Oxley)

FIGURE 1-2: The three domains of identity (IAM, PAM, and IGA) and how they interact.

REMEMBER

IAM is the foundational technology of identity. IAM performs the following important identity functions:

- Stores user data, policies, and configurations
- Manages user accounts and credentials
- Provisions and de-provisions users from applications and resources
- Authenticates users
- Controls access to applications
- Audits identities so you know who did what and when

Privileged access management (PAM)

Multiple users often need to share a unique account with privileged access for administrative tasks. For example, Linux has a super user account (root) that has privileged access and can do everything on a server. Other examples of super user accounts include the Windows Administrator account and Oracle Database's SYS user.

Because these accounts are not individualized, many organizations share the account credentials with multiple users (that is, all IT administrators know the root password), which is dangerous. Furthermore, it becomes challenging to know who did what and when, because although the server logs show that the root user deleted a critical system folder — who was using the root account at that moment? Thus, every IT administrator becomes a suspect.

PAM complements IAM with an intermediate vault. This vault keeps shared accounts with super user privileges secured with a random/secret password that no one knows. Each time a user needs to use a privileged account, they go to the PAM system to check the account out. Upon receiving a checkout request, the PAM system validates for how long a user can use that account, logs the checkout for audit, changes the super user account password, and then reveals the password to the user checking out the account. Once the authorized time has expired, the PAM system takes the account back (by changing the password to another secret value that no one knows) and stores it in the vault.

TIP

In addition to individual permissions, PAM is used to manage special types of accounts such as service accounts (used, for example, to interact with an operating system), application accounts (used, for example, to run a batch job or script), and database accounts (used, for example, to modify a database schema).

Identity governance and administration (IGA)

In the early 2000s, companies like Tyco, MCI WorldCom, and Enron manipulated their IT systems to report better financial results and increase their stock prices. Once these scandals were uncovered, a lot of stockholders lost a lot of money.

To prevent this from happening again, the government started to require companies listed on the stock market to control and better audit the accounts used in IT systems related to company finances. The controls included regularly reviewing who has access to what (in a process called *attestation*), as well as implementing request approvals and avoiding collusion (a process called *segregation of duties*).

To support some of these requirements, organizations can turbocharge their IAM with identity governance and administration (IGA).

REMEMBER

The need for IGA emerged in the wake of regulatory compliance requirements such as Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). IGA enforces attestation and segregation of duties, and also provides compliance reporting.

Whereas IAM and PAM are the technological pieces of identity, IGA can be thought of as the policy and process component of identity. IGA encompasses the policies that define:

- Who should be given access to what network resources based on their roles and responsibilities within the organization
- The organization's identity life cycle management processes (such as access requests and approvals, and account provisioning and deprovisioning)
- The ongoing verification of compliance with the organization's identity governance including logging, monitoring, and auditing identity and access

TIP

Many IGA systems also handle provisioning. However, modern identity solutions already incorporate these features natively (read Chapter 2 to learn more).

Looking at the Evolution of Identity

Like any other technology, identity has evolved over time to adapt to new challenges and requirements (see Figure 1-3).

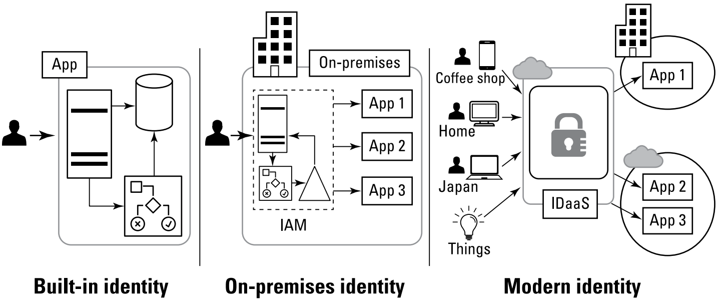

FIGURE 1-3: How identity is evolving to meet new IT and security challenges.

Built-in identity

In the beginning, identity consisted of local authentication to a mainframe or a desktop application. During this time, relatively few computers were connected, so organizations focused primarily on restricting local access to a workstation or application and protecting the operating system. As a result, many desktop operating systems and locally installed applications typically had basic built-in authentication capabilities requiring only a simple username and password to log in.

On-premises identity

In the mid to late 1990s, organizations began to interconnect computers and servers in LANs to share information. As Internet and web apps (such as email, intranet portals, Oracle, and SAP) adoption increased, so too did the requirement for more robust identity. Company networks grew to several thousands of computers, all being routinely connected to millions of services on the Internet, so organizations now had to deal with the threat of remote hackers breaching their networks. At the same time, user account management was becoming a real headache for IT, since users might need to log in to many different places including their desktop computers, dozens of apps, and their email clients. So there were now many places where IT had to control access and, of course, reset forgotten user passwords.

To solve these challenges, organizations started to manage identity on dedicated systems. Microsoft Active Directory (AD), first released with Windows 2000 Server, centralized network account management and enabled directory-based, identity-related services in Windows networks and apps. Similarly, Novell eDirectory (now NetIQ eDirectory) and Lightweight Directory Access Protocol (LDAP) enabled directory-based, identity related services in both Windows and non-Windows networks. And to secure access to web applications and emails, organizations adopted Web Single Sign-On solutions — also known as SSO or Web Access Management (WAM) — such as Oracle Access Manager, CA SiteMinder, PingAccess, Tivoli Access, and Microsoft Active Directory Federation Services (ADFS).

Identity as a Service (IDaaS) — also known as Modern Identity

Today, the need for robust identity management has never been greater. The risk of a breach or attack is constant and real, and the threat adversaries — from malicious insiders and cybercriminals to hacktivists and cyberterrorists — are highly motivated (typically by greed or ideology).

At the same time, there are more applications than ever before and they are increasingly being delivered as Software as a Service (SaaS) offerings in the cloud (for example, Office 365, Slack, and Zoom). According to the Okta 2020 "Businesses @ Work" report, the average number of apps per organization is currently 88, and the growth rate over the past 3 years has been 21 percent. Multiple devices of different types compound the problem further. In addition to a corporate issued laptop, virtually every user has, at least, an additional mobile device and a computer or iPad in their home. Many organizations don't necessarily control these environments — for example, AD can't control apps on Androids, Macs, and other non-Windows devices. Finally, users access applications and data from practically anywhere, including open (that is, not secure) Wi-Fi networks in airports and coffee shops.

TIP

To learn more about how organizations are using apps today, check out the "Businesses @ Work" report at `https://www.okta.com/businesses-at-work/2020/` and the Businesses @ Work Dashboard at `https://www.okta.com/businesses-at-work/`. This data is compiled in real-time and annually by Okta using anonymized data from thousands of customer organizations, applications, IT integrations, and daily user activity.

Thus, identity has not only evolved, but has more accurately morphed into a hybrid reality, where the apps being accessed, the device in use, and the network perimeter are always changing (imagine a world in which apes, Neanderthals, and homo sapiens all tried to work together on their computers and mobile devices while having coffee and bananas).

Traditional identity solutions like AD and on-premises SSO can't manage accounts and secure access in the face of all these trends and challenges. Even if they could, they would require hundreds of servers and hundreds of hours of work just to handle the load and requirements, which makes it almost impossible to solve these challenges with traditional on-premises identity solutions.

The solution is Identity as a Service (IDaaS), also known as modern identity — one identity to unite them all! You learn more about IDaaS in the rest of this book.

ADOBE USES OKTA TO CONNECT THOUSANDS TO THE CLOUD

In 2012, Adobe launched Creative Cloud and changed the creative world forever. The pivot moved all of the company's Creative Suite products to the cloud. A Creative Cloud membership would provide users with access to download and install every Adobe Creative Suite application.

Placing the whole creative workflow in the cloud fundamentally changed Adobe's business. Almost overnight, Adobe transitioned from perpetual product licenses and 18-month release cycles to monthly and yearly subscriptions and regular product updates.

It also changed Adobe's identity and access needs. The first release of Creative Cloud couldn't connect with the corporate identity systems that many of Adobe's enterprise customers already used. IT admins were having to set up and manage an entirely new set of user credentials within Adobe Creative Cloud, which created challenges down the road when users forgot a password or updated their credentials.

It didn't make sense for Adobe to custom build a scalable way to create federated connections between Creative Cloud and enterprise customers' identity systems. Engineering resources are better deployed to think up the next creative feature in Photoshop Creative Cloud or bring new connected creative mobile apps to market. "I don't want to reinvent the wheel in our identity stack. I want to use what's best in class in the market and then apply the Adobe-specific requirements to that stack to get something out to our customers really quickly," says Scott Castle, product manager for Creative Cloud.

Dual cloud challenges

Adobe's product team wasn't alone in dealing with authentication issues. By late 2014, the small internal IT team at Adobe was supporting some 300 cloud applications with an open-source single-sign-on solution they built themselves. That year, the company decided to deploy Microsoft Office 365 to all 13,500 Adobe employees — moving email, calendaring, and Sharepoint tools to the cloud. The old identity management platform, with its occasional quirks and outages, wasn't going to cut it.

Fortunately, says Den Jones, senior manager of IT services, it was around this time that the team was introduced to Okta. Working with an outside vendor made sense — one focused on securing and

(continued)

(continued)

authenticating apps in the cloud, rather than on building brilliant expressive design tools.

After reviewing their options and Okta's record in the industry, Adobe IT decided to sunset the internal single-sign-on system and deploy Office 365 with Okta authentication. After that roll-out, Adobe began moving the rest of its cloud apps to the Okta platform. Because maintenance for the old platform was up for renewal, the team was working on a fairly tight deadline: Three months to migrate 300 apps.

The timeline turned out to be perfectly reasonable, much to the delight of Jones and his team. It took about four weeks to get through the first 200 or more, he says. Today, most apps take minutes to provision, rather than the weeks or months it had taken before. Since then, Adobe has deployed multiple products from the Okta Identity Cloud across its growing employee base, securing and managing its workforce of 20,500 employees.

Identity for everyone

After working with Okta to secure employee access to cloud apps, Adobe IT was pretty clear about who the product team needed to work with to build enterprise identity into Creative Cloud for enterprise. Soon, Adobe engaged Okta to put the same powerful identity services into the hands of Adobe's product engineers.

Today, Adobe uses Okta to offer a comprehensive identity management layer to all its enterprise customers, including Adobe Marketing Cloud and Adobe Document Cloud, as well as Creative Cloud. The connected solution secures Adobe Cloud apps and lets users access Adobe's innovative tools with their existing corporate credentials — safely, quickly, and cost-effectively.

To make Creative Cloud users successful (and keep their customers' IT departments happy), Adobe's enterprise identity platform does a few very important things:

- Connects with customers' corporate identity systems — such as AD or LDAP — so IT admins don't have double the management activities
- Integrates Okta functionality into Adobe Creative Cloud's existing code
- Stands up with Adobe's branding on top
- Federates individual user identities with individual accounts, as well as multiple enterprise and agency accounts

IN THIS CHAPTER

- Introducing Identity as a Service (IDaaS)
- Solving modern identity challenges with IDaaS
- Using IDaaS for people and things

Chapter 2
Defining Identity as a Service (IDaaS) — The Modern Identity

In this chapter, you learn what IDaaS is all about, how it addresses modern identity challenges and its benefits, and how IDaaS supports use cases for employees, contractors, customers, and things.

Learning the Basics of IDaaS

Identity as a Service (IDaaS) is identity and access management (IAM) built and hosted by a service provider in the cloud, and available to organizations through a Software as a Service (SaaS) subscription. IDaaS solves modern requirements of identity without the limitations of the on-premises IAM model.

REMEMBER

By adopting SaaS solutions like IDaaS, organizations and IT administrators have realized the following benefits:

- **Faster time to value:** SaaS solutions are up and running by the time you sign up, eliminating tasks like procuring servers and installing software.
- **Fewer maintenance tasks:** SaaS solutions are constantly updated by their providers with new features and security improvements without outages, thereby reducing the number of maintenance tasks that must be completed by IT administrators.
- **Fewer manual integrations:** SaaS solutions are built with everything you need to get going, eliminating integration costs between internal components like servers, backup systems, and networks.
- **Cost flexibility:** Because SaaS solutions are typically charged per user per month, organizations can better control their spending and pay only for the services they are using.

These benefits are so significant that organizations are transitioning most of their core business to the cloud. If you're choosing a new IT solution for your organization today, it's harder to convince your bosses to buy servers, deploy data centers, install software, and have IT take care of all the maintenance than it is to subscribe to a cloud service.

REMEMBER

The goal of IDaaS is the same as IAM: to ensure users are who they claim to be, and to give them the right kinds of access to assets at the right times. The major difference is that IDaaS gives you the benefits of the cloud, without the limitations and overhead of on-premises IAM.

For an example, think about how you can provide Single Sign-On (SSO) using traditional on-premises IAM, such as Microsoft Active Directory Federation Services (AD FS) or Oracle Access Manager, versus IDaaS, such as Okta. As soon as you sign up for IDaaS and import your users, they all can benefit from the service. You don't need to spend your time and money buying and installing servers and operating systems or estimating the load and capacity for the service.

Furthermore, every time new functionality is introduced or an update is released — such as a new mobile app to secure access on Apple iOS and Android, or a security improvement to prevent access from the darknet — you get the updates automatically without requiring you to plan, test, schedule a maintenance window, and upgrade the system manually. Because IDaaS already has all the components required for managing identities, like multi-factor authentication (MFA) and provisioning, bolstering security is a snap and you don't need to buy, manually install, and integrate separate MFA or provisioning solutions from other software vendors or providers. Finally, you can control the service costs based on how people are using the service. So, for example, if you want to roll out MFA only for managers, you don't need to pay for MFA for all your employees.

IDaaS can be used to secure access and manage identities in different assets — including application programming interfaces (APIs), on-premises, cloud, mobile apps, and servers. It also provides multiple native capabilities, such as Adaptive MFA (discussed in Chapter 3) to improve authentication security, and SSO, which enables users to sign on to the network only once to obtain access to any of the applications and resources for which they are authorized.

In the on-premises universe, setting up all these capabilities (Adaptive MFA, SSO, directory services, and provisioning, among others) requires you to work across different servers, vendors (like Oracle, RSA, Microsoft, and Symantec), and manual integrations. With IDaaS, everything is available in a single offering, at scale, and with rapid time-to-value (see Figure 2-1).

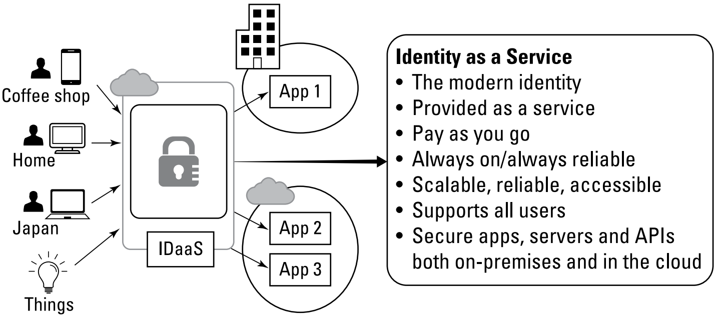

FIGURE 2-1: How IDaaS works with modern IT, and its benefits.

Addressing Identity Challenges

IDaaS solves many identity challenges that organizations must address today. IDaaS enables rapid integration with cloud and on-premises apps by leveraging open standards, like Security

Assertion Markup Language (SAML) and OpenID Connect (OIDC), and application catalogs. IDaaS also consolidates access control regardless of where an application is hosted, helping organizations running hybrid IT, with systems hosted in multiple on-premises, public cloud, and private cloud environments.

IDaaS provides the robust scalability, reliability, and accessibility that modern enterprises need in an always-on world in which potentially hundreds of thousands (even millions) of users — including employees, customers, and others — require access to their mobile apps, websites, APIs, and portals at any time and from any device.

REMEMBER

IDaaS provides many benefits for organizations, including:

- Improves an organization's cybersecurity posture with capabilities such as Adaptive MFA (discussed in Chapter 3) and centralized IAM.
- Increases user and IT productivity. Users can log in to all their applications faster with SSO and the IT help desk spends less time dealing with password resets. Whether a user is signing in from an open Wi-Fi network at an airport or from a desk in the office, the process is always seamless and secure.
- Helps an organization significantly reduce its IT costs. Provisioning identity onsite (for example, on Active Directory or Oracle Identity Manager), can be full of costs, including:
  - Purchasing, installing, upgrading, and maintaining server hardware (or virtual software licenses) and software
  - Paying hosting fees for space in a data center, private cloud, or public cloud
  - Configuring, maintaining, and monitoring virtual private network (VPN) connections

REMEMBER

With IDaaS, your only costs are the subscription fee and the IT administration work to manage your user accounts. Your user licenses can quickly and easily be scaled up or down to address the needs of your organization. IDaaS greatly reduces the recurring costs of running identity: from manual IT support requests for provisioning and resetting user accounts, to professional services for deploying, patching, and upgrading different solutions.

According to Forrester, "The biggest benefit of using IDaaS compared to on-premises IAM solutions is a 30 to 35 percent lower ongoing maintenance rate."

Exploring Use Cases

IDaaS supports many common business use cases for identity management (see Figure 2-2) such as employees, contractors, partners, customers, and things.

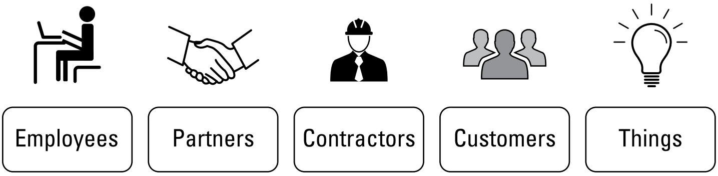

FIGURE 2-2: The use-cases (and users) that require identity.

Employees

Employees are the most important asset in any organization. Securely connecting your employees to the technologies they need is essential. Organizations today have employees accessing systems from anywhere working and collaborating remotely. At the same time, employees are being targeted by attackers looking to exploit their access.

IDaaS supports employees by:

- Onboarding and changing user access rights dynamically based on user data, informed by HR management systems like Workday and SuccessFactors
- Securely storing employees' identities and entitlements
- Securing employee access to all assets, including apps, servers, and APIs both on-premises and in the cloud, with a single set of strong credentials
- Enabling secure access regardless of user context, device, and network location
- Increasing employee efficiency by providing mobile-friendly access to the organization's assets

- Changing access requirements based on risk, dynamically denying or requiring MFA for high-risk access
- Rewarding "low-risk" users with password-less access
- Auditing and providing event information for the security team

Contractors and partners

Organizations work hard to build partnerships, but cumbersome processes and systems can stand in the way of effective collaboration. Partners and contractors introduce new, dynamic user types and create complexities for IT teams. At the same time, over-allocating access to partners exposes critical systems to unnecessary security risks.

Organizations have traditionally enabled contractor and partner access either by managing their identities using the same IAM solution as for their employees for short-term or relatively small relationships, or by integrating with their partner's own IAM stack, creating a business-to-business (B2B) integration for larger, long-term partner relationships.

Building B2B integrations is a costly and time-consuming undertaking. On average, the total cost of ownership of building and maintaining a B2B SAML integration, for example, in-house is $20,000 per integration.

TIP

IDaaS helps streamline the partner integration for both short-term and long-term B2B relationships. Benefits include:

- **Providing a seamless experience:** Integrate natively with your partner's IAM solution, allowing partners to access your resources with their existing credentials.
- **Encouraging collaboration:** Optimize partner experience by providing immediate access to the right resources via a personalized and secure portal.
- **Automating the partner life cycle:** Centralize user management and automate provisioning for partner identities to relieve administrative demands on IT.
- **Improving security:** Maintain total control of authentication, identity, applications, and resources and automate deprovisioning to prevent lingering access.

Customers and consumers

Today, every organization has a digital business via websites, APIs, and apps. Attracting customers and maximizing their lifetime value is increasingly dependent on meeting their high expectations for digital experiences that are technologically advanced, frictionless, omni-channel, and personalized.

Say you're shopping on Amazon or checking your photos on Instagram. Security in both examples is key, because you want to make sure nobody is buying things with your credit card and that your photos and comments are safe. However, if you have a cumbersome experience, it's unlikely you'll come back to these sites. You also expect to use the same login and have the same security and user experience on different devices. For example, you might use Instagram on both your computer and smartphone, and you might buy stuff on both the amazon.com website and via Alexa. Providing security without friction is the name of the game in consumer identity.

TIP

IDaaS can help organizations secure and deliver a superior customer experience in the following ways:

- **Improve the customer experience during registration and login:** Provide engaging, branded, and personalized experiences across channels. Easily customize the registration and login process across multiple apps without costly coding and development work.
- **Get a 360-degree view of the customer:** Overcome organizational silos created by disjointed accounts. By having a single identity per customer, organizations can understand that person's interests and preferences, increasing the customer's lifetime value.
- **Increase engagement:** Reduce onboarding friction with progressive profiling and password-less authentication. Seamlessly integrate apps into the customer portal for a single login experience.
- **Manage consent:** Give customers control over their data, and meet complex regulatory compliance requirements like the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). Learn more about consent management in Chapter 4.

Things

The Internet of Things (IoT) and the billions (already more than 30 billion in 2020) of smart, connected devices present new challenges for modern enterprises. Security in the IoT — with even greater threats to human life and public safety than other cybersecurity threats — is of paramount importance.

Smart things, such as Amazon Alexa, smart lightbulbs, and smart TVs, need identity for authentication and controlling what they can access and do — just like humans! However, there are many more smart devices than there are humans, and they communicate differently than humans — using APIs instead of browsers and apps.

REMEMBER

IDaaS provides the identity and scalability needed to meet the traffic demands of IoT. Furthermore, IDaaS supports the protocols expected by smart IoT devices — such as Open Authorization (OAuth) — to secure access to APIs.

WHAT IDaaS ISN'T

This chapter covers what IDaaS is. In a nutshell, IDaaS is a cloud-based IAM solution that secures access to applications and systems for an organization's users, including employees, contractors, partners, customers, and things.

So, what *isn't* IDaaS? Well, for starters, an on-premises identity management solution that has been migrated to the cloud in an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) offering, isn't IDaaS. Lifting-and-shifting your on-premises Active Directory servers to a PaaS solution, or even adopting a modern container technology like Docker, for example, still keeps you responsible for manually installing and patching systems, doing capacity planning, and integrating manually with other modules or vendors — and all without the pay-as-you-go benefit of a true IDaaS. Therefore, this isn't IDaaS. Even though containers are super cool (especially for building your own apps), all you've accomplished is moving your on-premises challenges to the cloud!

Also, IDaaS isn't a managed service provider (MSP) solution. MSPs typically run a legacy IAM on your behalf while charging you a subscription fee. Even though these solutions reduce your maintenance burden, they don't eliminate key limitations of traditional IAM, such as getting real-time upgrades without planned outages or providing thousands of out-of-the-box integrations to mobile apps, cloud apps, and APIs.

IN THIS CHAPTER

- **Looking at the building blocks of Identity as a Service**
- **Controlling access to different resources**
- **Considering integrations, security and privacy, compliance and more**

Chapter 3

The Building Blocks of Identity as a Service

In this chapter, you learn about the key components of Identity as a Service (IDaaS), the resources that can be secured with IDaaS, and key considerations you need to keep in mind when adopting an IDaaS solution.

The Building Blocks

IDaaS solutions typically have four main building blocks:

- Directory
- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Provisioning and workflows

Directory

Directory is a critical component of any identity and access management (IAM) solution. This is a database of entities (users, groups, and resources), metadata (configurations and policies), and audit data required by IAM to do its job.

Microsoft Active Directory (AD) is an example of a traditional directory installed in an on-premises environment. Others include Apache DS, NetIQ eDirectory, OpenLDAP, and Oracle Internet Directory (OID).

Traditional on-premises directories were built before the cloud, remote workforce, increased merger and acquisitions (M&As) and business-to-business (B2B) activity, and the smartphones/app revolution. These directories thus are not fully optimized to deal with modern requirements. When organizations force-fit on-premises directories to meet modern requirements, such as to support cloud apps or manage mobile devices, they end up deploying multiple directory forests, trees, trusted domains, servers, custom integrations, and PowerShell/bash scripts, creating extremely complex environments that ultimately do not meet their needs.

REMEMBER

A modern solution must address modern requirements and integrate seamlessly with the systems that will use the directory without requiring you to deal with manual integrations and complexity.

IDaaS solutions deliver a built-in directory that securely stores the data required to address all modern use cases — from mobile to M&A and cloud — without requiring you to take care of the infrastructure or deal with custom setups, PowerShell, or bash scripts. The directory is natively integrated to all services that will consume it, such as SSO for authenticating users, eliminating manual integration tasks.

TIP

When adopting a modern IDaaS stack, many organizations look at decommissioning their on-premises directories. Retiring legacy directories is a snap in deployments where the directory is used exclusively for IAM. However, retiring a directory in complex environments requires planning. For example, in many organizations Active Directory (AD) stores not only identity, but is also used for services like domain name system (DNS) resolution and for issuing private key certificates. Moreover, some companies develop custom PowerShell integrations or cobble together hundreds of domain controllers to store their data. The best practice for complex deployments is to reduce legacy directory usage by moving services to modern solutions while reducing complexity.

For example, by using an IDaaS solution with a built-in directory and provisioning, you can eliminate custom PowerShell scripts for identity-related activities like bringing employees onboard during an M&A or synchronizing email addresses across many systems. Offloading these tasks to IDaaS drastically reduces the number of servers and complexity in your on-premises directory.

Single Sign-On (SSO)

Login credentials exist to keep accounts secure, but they pose a challenge because users have different accounts in hundreds of applications. To keep up with all these apps while avoiding password fatigue and lost productivity, users take dangerous shortcuts like reusing credentials across all apps or writing passwords on notepads or in spreadsheets. Verizon has found that stolen credentials are the most common source of data breaches, and it's fair to say this is largely because users struggle to manage their many credentials.

SSO solves this challenge by allowing access to all apps with a single login. To accomplish this, SSO relies on open standards like Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to federate users to third-party systems and apps.

TIP

SSO solutions are sometimes criticized for introducing a single point of failure into the authentication process, something people refer to as "keys to the kingdom." However, there are important features and best practices that not only address this concern, but also boost security and productivity. Here are some examples:

- **MFA:** MFA is considered the best friend of SSO. The use of MFA boosts SSO security with authentication via additional factors, like user biometrics, that are more secure than traditional passwords.
- **Adaptive access:** A good practice for boosting SSO security is to use solutions that re-evaluate user access based on their context, network, device, and location, and leverage intelligent threat feeds. In this way, SSO automatically changes the login requirement, blocks access, and triggers security alerts when suspicious events occur.

SSO is a great way to enforce strong password practices for your users. With just one password to control, IT can set policies to make sure that password is as secure as possible, including requirements that passwords:

- Expire after a certain amount of time
- Differ from previous ones to prevent reuse

- Do not match an existing list of hacked credentials
- Lock after a certain number of unsuccessful attempts to protect against brute-force attacks

TIP

Password managers can also facilitate access for end-users, but password managers focus on protecting credentials in a vault (instead of eliminating passwords). Moreover, password managers do not implement key security features such as the ability to look at the user's context or the ability to prevent access from malicious networks.

With these capabilities, even if a user enters the correct credentials, the user may have a limited session (with a timeout in minutes instead of hours), be asked for additional authentication, or have the access completely denied. For example, if a user is using a Tor anonymizer to log into a sensitive system, access can be completely denied. SSO gives administrators more control and granularity over how users are given access to company resources.

TIP

Read the Okta myth-busting series to learn more about SSO at `https://okta.com/blog`.

Adaptive Multi-Factor Authentication (MFA)

Authenticating a user typically involves validating an identity claim (such as a username) with what's known as a *factor.* Authentication factors are generally considered to be one of three types:

- **Something you know** — such as a personal identification number (PIN), password, or your mother's maiden name
- **Something you have or possess** — such as a smartphone, your employee badge, or Fast ID Online Universal Second Factor (FIDO U2F) key
- **Something you are** — a unique biometric identifier such as a fingerprint, retina, or iris pattern

Most applications authenticate users against a single factor, typically a password. Using passwords, although simple and straightforward, has plenty of disadvantages. Passwords are the easiest way to break into your systems and hackers can take advantage of them in multiple ways.

TIP

The top five password attacks are: broad-based phishing, targeted spear phishing, credential stuffing, password spraying, and man-in-the-middle. To learn how these attacks are carried out, check out `https://www.okta.com/resources/whitepaper/5-identity-attacks-that-exploit-your-broken-authentication/`.

TIP

You can use free resources like `https://haveibeenpwned.com/` and the PassProtect plugin for the Google Chrome browser to see if your passwords and accounts have been compromised.

TECHNICAL STUFF

Passwords are also subject to brute-force attacks. However, most systems can block these attacks by using an account lockout safeguard after a certain number of failed login attempts.

The solution to the inherent weaknesses and challenges in passwords and single-factor authentication is — multi-factor authentication (MFA)!

MFA requires two or more factors to authenticate an identity. For example, MFA might require a user to log in to a website with a password, then enter a one-time passcode that is sent to the user's smartphone. The passcode is valid for a limited time (typically three to five minutes) and can only be used for one login attempt. If the passcode is incorrectly entered or the user logs out of the session and tries to log in again using the same passcode, the login attempt fails.

The downside of MFA is that requiring it every time a user logs in can cause MFA fatigue. MFA introduces friction to the end-users, who may need to re-authenticate throughout their workday or use a combination of both hardware and software tokens to gain access. Every additional authentication factor required improves access control, but at the expense of making your user experience less friendly. However, MFA friction can be mitigated by reducing the number of times that users need to login (with — you guessed it — SSO!), by using more seamless and intuitive factors, and by making your MFA adaptive to different contexts and risk profiles.

To balance security with cost and usability, IDaaS provides extensive support for different MFA factors. These factors range from low assurance, such as security questions and short message service (SMS) text codes, to high assurance, such as push notifications, biometrics, and hardware tokens.

TIP

Many organizations still rely on low-assurance factors like security questions and SMS text codes. Security questions are the most popular factor that organizations use today, and it's on the rise. According to research by Okta, 38 percent of MFA users today are using security questions as a second factor, compared to 30 percent last year. The problem with security questions is that the answers to these questions can often be found in public records and on social media (for example, your mother's maiden name or your spouse's name). Using SMS text messages as a sole second factor also comes with risk. For organizations that must comply with regulations like the Defense Federal Acquisition Regulation Supplement (DFARS), the U.S. National Institute of Standards and Technologies (NIST) guidelines no longer allow SMS-based two-factor authentication because of the risk of codes being intercepted. This doesn't mean these factors are ineffective in an MFA solution. Instead, the right factors must be paired with the right level of risk.

To improve security without increasing friction, IDaaS implements adaptive MFA. Adaptive MFA analyzes individual login requests using backend analytics to determine how many factors to prompt for and how much access to grant. For example, if an employee is working on the company premises and uses a smart badge to get through security to her office, adaptive MFA recognizes that she is in a trusted location and may only require her fingerprint to log in to the system. However, if that same employee is working on a personal device from a coffee shop, adaptive MFA may prompt her for an additional authentication factor.

Provisioning and workflows

Up to this point, you've learned about three building blocks of IDaaS: Directory keeps user data and configurations in place, SSO reduces user friction for access to hundreds of systems and applications, and Adaptive MFA bolsters user security for access to all apps based on their level of risk. But there's one final challenge: How do you make sure your users are correctly added to your IDaaS directory and they are provisioned to the systems they need in order to log in? Provisioning and workflows solve this challenge.

With provisioning, organizations can use IDaaS to not only control access to systems, but also to create, update, and delete accounts and privileges based on the status of their users. The user status can be defined directly in the IDaaS directory or in important third-party systems that are considered the source of truth for the organization (for example, the best source of truth for employees in the organization might be the human resources system).

Provisioning automates the account and privilege management of internal and external accounts, thereby saving time and money. On average, organizations save 30 minutes on every application provisioning request, 30 minutes determining and configuring groups and entitlement, and $20 per user preparing for audits each year. When multiplied across the thousands of provisioning requests and various audits that the typical organization must deal with every year, the time and cost savings can be quite significant.

However, other processes beyond account management must also be triggered in third-party systems due to changes in identity. For example:

- Martin joins the security team. In addition to getting access to the security systems, Martin needs to complete a security training course (for example, in Udemy) and sign a document (perhaps in Adobe Sign or DocuSign) confirming that he understood and completed the course.
- Yara, a customer living in Germany, accesses your company's shopping app and submits a request for a copy of all her personal data collected by your company. The European Union General Data Protection Regulation (GDPR) requires your company to provide Yara a copy of her data within 30 days.

Workflows is an IDaaS capability that provides automation beyond account provisioning, allowing you to automate and orchestrate these types of processes without requiring additional code to be written.

REMEMBER

IDaaS delivers all the building blocks of IAM — Directory, SSO, Adaptive MFA, and provisioning and workflows — in a single and cohesive package, all up and running for you as soon as you subscribe to the service. This allows you to get the best time to value and focus on important things like setting up security and improving user experience while saving time and money, instead of installing, patching, and integrating disjointed solutions.

Resources

In this section, we describe some of the main types of resources you can secure access to and manage identity for with IDaaS directory, SSO, Adaptive MFA, provisioning, and workflows.

Cloud apps

Many cloud applications — such as Office 365, Salesforce, Amazon Web Services, and Slack — exist. In fact, the cloud is becoming the predominant delivery model for applications, quickly supplanting locally installed software as the preferred method. Modern IDaaS solutions give you a catalog of pre-built app integrations. You can use the catalog to integrate with your cloud apps in minutes.

TIP

The integrations between IDaaS solutions and cloud apps are done through open-standards like SAML for federation and System for Cross-domain Identity Management (SCIM) for provisioning.

TIP

Okta currently has more than 6,000 pre-built app integrations.

On-premises apps

Although companies are increasingly adopting an ever-growing number of cloud apps and services, most organizations keep at least some of their systems running on-premises. Modern IDaaS solutions offer capabilities to secure access to on-premises web applications, using traditional on-premises integration patterns and standards like Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), Kerberos, and header-based authentication, without requiring changes to the application source code.

TIP

You can use the same IDaaS solution to protect all your systems — from ground to cloud — using the same security policies, saving you time and money while always leveraging the latest security features.

Custom apps

As Mark Andreessen, founder of Netscape, famously wrote nearly a decade ago, “software is eating the world.” Every organization today is, at some level, a “tech company” building a digital presence for itself, whether it’s e-shopping, a ride-sharing app, or the next big thing. Software innovation is “table stakes” for organizations to survive in today's hypercompetitive global economy.

Look around in your own company. How many app developers do you have today compared to just five years ago? If you're in a truly innovative, leading-edge company, you likely not only have more developers; you have more *types* of developers including mobile app developers, data scientists, and machine learning engineers. All these people are building custom apps that require security, but they aren't necessarily (or even likely to be) security specialists. Delivering an insecure app subject to account takeovers or credential compromise can cost an organization a fortune (if not everything) resulting from litigation, fines and penalties, adverse publicity, brand reputation damage, and loss of customer trust and business opportunities.

IDaaS provides built-in SSO and MFA in the form of software development kits (SDKs) and APIs that developers can quickly and easily add to their apps so that developers can focus on what they do best — building apps — while having best-in-class directory, SSO, MFA, and provisioning and workflow security.

Servers

Software has to run somewhere, and that somewhere is usually on servers that may be hosted in multiple places — including an on-premises data center, a private cloud, or a public cloud such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure. With modern architectures and app dev tools like microservices, containers, serverless, Kubernetes, and DevOps, the number of instances running your application can vary dynamically based on load. For example, a new app might be launched on just ten servers running in a public cloud, and within hours of going viral you may have more than 1,000 servers in your cloud infrastructure that have been provisioned to handle the load. Imagine trying to secure all these servers yourself as they quickly scale up and down. Modern IDaaS solutions provide a way for you to secure access to all your servers and application instances automatically.

Application programming interfaces (APIs)

APIs are the fuel for all that software that's eating the world. You can think about APIs as an app that can be consumed by other apps and Internet of Things (IoT) smart devices. APIs save developers time by not requiring them to build functions that someone else has already created. Some examples of what you can do with APIs include using:

- Twilio to send SMS text messages to a smartphone
- Stripe to process credit card payments
- Google Analytics to track visits to your website

Also, as an organization, you can join the API economy: Build your own APIs, offer it for other organizations to use for their apps, and make money out of requests. For example, if you're a shipping company, you can offer an API to calculate delivery time, shipping costs, and to request shipping labels.

Modern IDaaS solutions secure and authorize access to APIs, leveraging API security standards like Open Authorization (OAuth).

And many other things . . .

Sometimes you have IT resources that require identity but are not classified as a cloud app, an on-premises app, a server, a custom app, or even an API. In these situations, you can still benefit from the identity security of IDaaS through open standards. Open standards and patterns are used in many industries (including IT) to provide seamless integration between systems.

Without standards, just about everything in the world would be more difficult. Imagine trying to buy a lamp if every manufacturer had their own proprietary light bulbs that only worked in their lamps, or using a phone if everyone you knew had a different length phone number, such as 22 digits, 15 digits, 11 digits, or just one digit!

Identity, like any other industry, has standards. There are identity standards for everything: from directories (such as LDAP) to authentication and SSO (for example, SAML, RADIUS, and OIDC), to provisioning and workflows (for example, SCIM and Representational State Transfer [REST], and Webhooks). IDaaS leverages these standards to support a variety of systems.

REMEMBER

Standards allow you to implement best-of-breed solutions and help you avoid vendor lock-in with proprietary solutions. Vendor lock-in restricts the flexibility of your business. You're stuck with whatever the vendor wants to charge you for ongoing maintenance and support, and you're limited to the features and capabilities that they deliver in their product road map (if they even *have* a road map). Switching to a different solution when you've had enough can be quite costly (for example, how do you get your data out of the old system and into the new one?).

TIP

Download the Integration Patterns for Legacy Applications e-book at https://okta.com/resources/whitepaper-integration-patterns-for-legacy-applications and read the Okta blog at https://okta.com/blog to learn more about standards and integration.

Other Important Considerations

Identity is a mission-critical component in your IT. If your identity system is not running, people lose access to multiple resources. If your identity solution is not secure, your entire organization is exposed to substantial risk. To choose an IDaaS solution that won't let you down or lock you in, you must consider additional factors. These include integrations, neutrality, security and privacy, compliance, and availability.

Integrations

Third-party integrations are a key consideration for organizations looking at IDaaS. A broad ecosystem of integrations helps you seamlessly enable SSO, avoid vendor lock-in, and unlock new value from existing applications and IT systems. An IDaaS solution should support the apps you use today and that you're considering using in the future, via a catalog of integrations. Also, the solution should provide a rich set of integrations beyond SSO, including:

- **Login and provisioning:** Enables you to control access and provisioning to applications, such as Box, Office 365, Salesforce, ServiceNow, Slack, and Zoom, in minutes. The integration should go beyond SSO and support user provisioning, offboarding, advanced integrations via workflows, device, and license management options.
- **Human resource information systems (HRIS):** Connect to HR systems like Workday and SuccessFactors to automate employee onboarding and offboarding.
- **Application delivery controllers (ADC):** Connect external users to on-premises ADCs such as Citrix, F5, and Akamai.

- **Network security:** Extend SSO and MFA to corporate network security solutions like Cisco, Check Point, Palo Alto Networks, and ZScaler.
- **Security analytics:** Expand your view across cloud, mobile, and on-premises systems to amplify correlation and enforcement opportunities. Examples include LogRhythm, Rapid7, QRadar, and Splunk.

TIP

Okta publishes its app catalog at `https://www.okta.com/okta-integration-network/`.

Neutrality

Using open standards and providing integrations — both discussed in the previous sections — in a Modern IDaaS solution is important, but it isn't enough. An IDaaS service provider must be neutral. That is, your service provider needs to provide clear evidence that it doesn't pick favorites among solutions that it works with, thereby indirectly locking you into one vendor or another. For example, Microsoft, NetSuite, Salesforce, and Zoho (notice we didn't play favorites in the order we listed them — they're alphabetical!) all provide great customer relationship management (CRM) software and all compete against each other. A modern IDaaS solution needs to support as many popular software options as possible within any given category.

TIP

Look for the following signs of neutrality in a modern IDaaS provider:

- A broad ecosystem (at least 5,000) of native integrations to IT systems and software
- Deep integrations, even with competitive products from the vendors offering a particular solution
- Broad support for open industry standards

TIP

Okta supports a broad range of vendors and solutions listed on `https://www.okta.com/oin/`.

Security and privacy

Security and privacy are top-of-mind for every organization today, and your modern IDaaS provider is no different. Look for the following security and privacy assurances in your IDaaS provider:

- Documentation of their security (that is, confidentiality, integrity, and availability) controls.
- Support for the cloud shared responsibility model clearly outlining what they are responsible for and what you are responsible for.
- Documentation, best practices, and product features to help you secure your service instance.
- Evidence of a solid track record in security and privacy. Your IDaaS vendor should provide tools and evidence such as trust portals, public bug bounty programs, and automated security testing.
- The right to test the security of their IDaaS platform and solution.
- Certifications such as Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR), Federal Risk and Authorization Management Program (FedRAMP), International Organization of Standardization (ISO) 27001, and System and Organization Controls (SOC) 2 Type 2.

TIP

For information about Okta service security, check out the whitepaper at `https://www.okta.com/resources/whitepaper-okta-security-technical-white-paper`.

Compliance

Organizations in different industries have different regulatory compliance requirements. Ensure your IDaaS solution meets any regulatory requirements or industry standards that may be applicable to your organization. These might include, for example, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and others. Relevant standards might include the Payment Card Industry (PCI) Data Security Standards (DSS) and the International Organization for Standardization (ISO) 27001 standards.

TIP

You can learn about Okta's compliance approach and certifications at `https://trust.okta.com/compliance`.

AN IDAAS EXAMPLE: HOW OKTA DOES IT

The Okta Identity Cloud is the IDaaS platform built and maintained by Okta. As a true cloud-native service — 100 percent born and built in the cloud, Okta provides key benefits, including:

- It's globally available, 100 percent multi-tenant, stateless, and redundant.
- It's regularly updated with security enhancements and new features.
- It has zero planned downtime; Okta updates the platform on-the-fly and doesn't schedule downtime for maintenance.
- It drastically reduces operational tasks and setup and maintenance costs.
- It's subscription-based and cost-flexible.

These benefits are rarely found in on-premises software, managed cloud services, or at vendors that ported legacy on-premises software to the cloud.

The Identity Cloud Platform features include both Workforce and Customer Identity products.

Workforce Identity

Workforce Identity products are geared toward IT and security leaders. At a very high level, they simplify the way people connect to enterprise technology, while increasing efficiency and helping keep IT environments secure. These solutions include:

- **Universal Directory:** Customize, organize, and manage any set of user attributes from multiple identity sources with this flexible, cloud-based user store.
- **Single Sign-On:** Free your people from the chains of multiple passwords. A single set of credentials gives them access to enterprise apps in the cloud, on-premises, and on mobile devices.
- **Lifecycle Management:** Automate user onboarding and offboarding by ensuring seamless communication between directories such as Active Directory and LDAP, and cloud applications such as Workday, SuccessFactors, Office 365 and RingCentral.
- **Adaptive Multi-Factor Authentication:** Secure your apps and virtual private network (VPN) with a robust policy framework, a

comprehensive set of modern verification factors, and adaptive, risk-based authentication that integrates with all of your apps and infrastructure.

With Workforce Identity, IT enjoys one central place for policy-based management that governs which users get access to the mission-critical applications and data that power core business processes.

Employees benefit from a single sign-on home page that simplifies their lives and reduces security risks caused by "password fatigue." With Okta, they no longer resort to risky practices for memorizing passwords — for example, by choosing obvious or reused passwords, writing passwords down on Post-it notes, or saving them in Excel files on their laptops.

Customer Identity

Customer Identity products allow you to embed Okta as the identity layer of your apps or customize Okta in order to:

- **Deliver a customizable user experience:** Leverage Okta APIs and widgets to create fully-branded login flows or end-user portals. You can even use Okta's APIs to build a custom admin experience where customers or division managers can manage their users.
- **Extend Okta to any use case:** Solve any complex identity integration, data or automation challenge by taking advantage of Okta's broad APIs. Run scripts to modify user data, automatically integrate apps, or integrate with custom workflows.
- **Leverage the best-in-class customer IAM (CIAM) solution:** Free your developers to focus on the customer experience and leave identity to Okta. Leverage Okta as an "identity API" for all your app dev projects, with Okta handling authentication, authorization, and user management.

Customer Identity products provide programmatic access to the Okta Identity Cloud, enabling your developers to build great user experiences and extend Okta in any way you can imagine. By powering customer identity for your digital business, Okta can solve your most complex enterprise architecture challenges.

Enterprises that adopt the Okta service dramatically improve the security and experience for users interacting with their applications — whether they are employees, contractors or customers, using a cloud service, on-premises application, VPN, firewall, or custom app.

Availability

An IDaaS provider must ensure the service is always available to ensure your organizations employees and customers can log in anytime, from anywhere, and from any device.

Look for an IDaaS provider with a robust cloud architecture, comprehensive service-level agreements (SLAs) that meet your business requirements, and a public dashboard with real-time monitoring and status information about the service.

TIP

Okta publishes its service availability in real time at `https://trust.okta.com`.

IN THIS CHAPTER

- » Going from zero to Zero Trust
- » Leveraging blockchain technology
- » Exploring identity challenges and solutions on the Internet of Things (IoT)
- » Addressing privacy concerns
- » Looking at best-of-breed applications

Chapter 4

Looking to the Near Future of Identity

In this chapter, you look at what the near future holds for identity and how modern identity helps you stay current with coming innovations.

Zero Trust

The ubiquity of mobile and cloud computing has rendered the notion of a network perimeter — with a "trusted" internal network and an "untrusted" external network — all but obsolete. In this new reality, organizations must securely enable access for their users regardless of location, device, or network.

To solve these challenges, John Kindervag created the Zero Trust security framework while at Forrester Research in 2010. Zero Trust is based on the principle of "never trust, always verify," meaning the right people have the right level of access to the right resources in the right context — and that access is continuously assessed. Thus, identity and access management (IAM) is a core technology and a linchpin in the Zero Trust framework and should be the starting point for organizations that are implementing a Zero Trust architecture.

TIP

Forrester Research has named Okta a "Leader" in its report, "The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019." Okta earned the highest possible score across half of the evaluation criteria .

Decentralized/Self-Sovereign Identity

In a decentralized or self-sovereign identity model, individuals manage their digital identities themselves. This model gives the individual greater control of their accounts and data. A self-sovereign identity has three components: a *claim,* in which the individual asserts their identity; *proofs* — such as a block in a blockchain — used to provide evidence that a claim is valid; and an *attestation,* in which a system validates the claim based on the proof presented.

A common example of self-sovereign identity today is Apple FaceID, which is used on iPhones to access the phone, make online purchases, and log into various apps. The claim is stored locally on the device when FaceID is initially set up for the iPhone owner. The proof is the set of unique facial characteristics of the user, which have previously been registered with the claim as part of the setup process, and the attestation is the FaceID software's automated verification of the claim and proof.

Internet of Things (IoT)

The Internet of Things (IoT) refers to the network of "smart" devices that are embedded with electronics, software, sensors, and network connectivity to enable advanced capabilities and features. Although the IoT delivers many innovations, it also presents a far greater risk to access control and data.

So, what does the IoT mean for IAM? Clearly, IoT devices need to be properly identified and authenticated, and the cloud is the only platform that provides the robust scalability necessary to support directory services and access control for tens of billions of devices worldwide.

TIP

It also turns out that IoT can be part of the solution. IDaaS solutions can leverage wearables, such as the Apple Watch, as a factor in adaptive multi-factor authentication (MFA), providing push notifications to authenticate access requests.

Privacy at Global Scale

Privacy regulations such as the European Union (EU) General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Australian Privacy Principles (APP) have defined greater privacy rights for individuals and present growing legal and compliance challenges for organizations worldwide.

One aspect of many privacy regulations is the requirement for consent data (such as legal agreements and marketing information) to be collected, periodically reviewed and re-confirmed by consumers, and provided for a specific processing purpose. Additionally, when consent is given, organizations must ensure that only the minimum data that is needed is collected, and that it is only used for lawful and authorized processing purposes. Adding further to this complexity, some consents (such as marketing requests) can be revoked by the user, while others, such as legal agreements, cannot.

Managing consent requires organizations to track multiple regulations and customer data recorded in multiple systems and databases. Solutions like customer data platforms (CDP) and IDaaS help aggregate customer data and simplify consent handling across multiple sub-processors and systems.

TIP

As more countries enhance their consent requirements, consent management will require solutions to support privacy at global scale.

Identity Freedom

As the enterprise software ecosystem grows and becomes more heterogeneous, enterprises are looking for the best applications to support their workforces and increase efficiency, all while maintaining control and security. Organizations are increasingly deploying best-of-breed applications, such as Slack and Zoom, alongside full application suites, such as Office 365 — even when their capabilities overlap.

TIP

As of June 2019, more than 77 percent of Okta's customers with Office 365 had also adopted best-of-breed applications, such as Slack, Zoom, Box, AWS, Salesforce, or G-Suite, and these numbers have been steadily growing. Between October 2018 and June 2019, Zoom saw a 25 percent increase in Office 365 customers adopting its solution, the most of any best-of-breed app analyzed within Okta's customer base. Slack's growth among Office 365 customers was also in double-digit territory, rising from 11 percent to 31 percent, which indicates the race is on for best-of-breed collaboration apps in the enterprise.

Although users within an organization often quickly adopt best-of-breed applications, one significant inhibitor can be identity and access. To promote best-of-breed and avoid vendor lock-in, users need an IDaaS solution that secures access for any app, regardless of vendor or provider.

How IDaaS Correlates with These Trends

The world is in a constant state of change, but one thing everyone knows for certain is that new IT innovations, threats, and ways of securing identities will continue being developed. IDaaS, is built from the ground up to support changes today and in the future. Unlike legacy identity and access management solutions, IDaaS:

- Enables Zero Trust by securing access for users regardless of location, device, or network
- Supports open standards and connects to systems that provide self-sovereign identity
- Secures and authorizes access to application programming interfaces (APIs) used by smart devices and scales to the needs of IoT
- Aggregates customer data and simplifies consent handling across multiple sub-processors and systems
- Provides identity freedom so organizations can adopt best-of-breed technologies and avoid vendor lock-in

REMEMBER

With IDaaS, you get a flexible linchpin that you can easily connect to and deploy new innovations for your organization today and in the future.

PERSONAL CAPITAL MANAGES ITS CLOUD ENVIRONMENT

Personal Capital offers a "high-tech, high-touch approach to personal investing," bringing financial clarity and confidence through the combined power of smart technology and smart people. As of February 2019, the company managed more than $9 billion in assets and more than two million customer user accounts.

To support the growth and scale of the business while keeping financial data secure, Personal Capital operates a robust cloud architecture. Initially, the company's identity management strategy was overly complex, said Maxime Rousseau, chief information security officer.

Solving for Zero Trust infrastructure access

Personal Capital runs both customer-facing applications and backend services on Amazon Web Services (AWS). After successfully deploying Okta, the next step was to secure access to their cloud infrastructure.

The team committed to the Forrester Zero Trust model, where access is granted according to dynamic, real-time user and device conditions. "We're a modern, cloud-first organization with no traditional perimeter, and that's how we believe security should work," said Rousseau.

Providing that level of oversight was no easy task, however. "It was a challenge to dynamically provision the right identities, roles, groups, and associated public Secure Shell (SSH) keys while spinning immutable infrastructure up and down at scale," said Rousseau. Without a unified layer for access control, the team had to either build their own connective tissue or add bolt-on access technologies on top, which would present adoption, compatibility, and scaling issues.

An auspicious and timely acquisition

To leverage Okta's authentication stack, the Personal Capital team opted for ScaleFT and its Zero Trust Server Access product, which was integrated with Okta, providing dynamic provisioning capabilities. ScaleFT gave Personal Capital's operations, security, data science, and engineering teams a seamless, secure way to access critical AWS infrastructure.

At the time, ScaleFT was going through the formal process of verifying its Okta integration, and the company needed a joint Okta and ScaleFT

(continued)

(continued)

customer to confirm that the integration was working as documented. Personal Capital volunteered to be the mutual customer and helped finalize ScaleFT's Okta verification. "We were one of the first client bridges between the parties," said Rousseau.

After verification, Okta took the partnership further and announced in July 2018 that the company would acquire ScaleFT to extend identity to infrastructure resources and accelerate the roadmap for its Zero Trust platform.

That announcement was great news to the team at Personal Capital. Today, the ScaleFT Server Access product is called Okta Advanced Server Access. It streamlines core Okta authentication workflows to Linux and Windows servers via SSH and Microsoft's Remote Desktop Protocol (RDP).

Zero Trust — made friendly, as well as secure

"Okta Advanced Server Access was the right choice for Personal Capital because it simplifies secure server access while eliminating the need for additional technologies, manual integration and static keys," said Rousseau. By solving for all policy requirements with one technology, Personal Capital avoids brittle manual integrations.

Advanced Server Access delivers a Zero Trust architecture that protects Personal Capital's critical infrastructure. "Like Personal Capital, Okta ties everything to identity," said Rousseau. "Advanced Server Access binds user devices to authenticated sessions, so we have added assurance that each device and employee can be trusted, at each point in time."

Advanced Server Access removes much of the traditional operational burden that comes with infrastructure. "We have no account synchronization to worry about, no static credentials that can be stolen and/or misused," said Rousseau. "We can see who accessed what, from which machine, and when."

As Personal Capital continues to lead the digital wealth management space with advanced technologies, Rousseau feels confident that the company's infrastructure is prepared. "With Okta covering identity and access management, we have a secure, scalable foundation on which to grow," he said. "Okta was the right choice for us."

IN THIS CHAPTER

- Keeping identity simple . . . and vendor neutral
- Doing more than access control for any user
- Leveraging a cloud service model
- Replacing legacy products with a scalable, secure, and user-friendly solution
- Preparing for the future

Chapter 5
Ten Key Capabilities of Modern Identity as a Service (IDaaS)

Here are ten important capabilities and business benefits of a modern Identity as a Service (IDaaS) solution:

- **It's simple to deploy and use.** With a cloud-based Identity as a Service (IDaaS) solution, you can deploy identity and access management (IAM) in hours and integrate with applications in minutes, not weeks. By the time you subscribe to the service, the solution is already up and running. No server installation is needed.
- **It's vendor-neutral.** IDaaS integrates with apps universally. It supports cloud and on-prem apps, custom apps, mobile apps, servers, and APIs, via a catalog with more than 6,000 pre-built integrations, preventing vendor lock-in.

- **It goes beyond access control.** IDaaS provides multiple services in one solution. This includes storing user data, providing self-service account recovery and access requests, automating account provisioning and cutoffs, implementing workflows, and simplifying security auditing. These capabilities eliminate manual tasks performed by IT, reducing overall costs.
- **It supports all users.** IDaaS can manage all users in a single platform. It reduces the systems and vendors required to secure identities and the number of integrations an app needs to support all users.
- **It enables pay as you go.** IDaaS is subscription-based. You pay as you grow. You can quickly change the number of licenses needed as your business changes, providing cost flexibility.
- **It's always on and up to date.** IDaaS is updated regularly by the service provider with security improvements and new features, without outages or downtime. The service also provides real-time availability on a live dashboard, allowing you to focus on strategical projects instead of manually patching systems.
- **It's a way out of legacy solutions.** IDaaS replaces multiple legacy identity solutions from LDAP, Microsoft Active Directory, and Active Directory Federation Services (AD FS) to on-premises SSO and MFA servers. Replacing these systems with a unified service saves you time and money associated with vendor management, procurement, manual integrations, patches, maintenance, and support.
- **It's scalable and flexible.** IDaaS dynamically scales for demand, so you don't need to forecast, install, and patch infrastructure for your company's growth for upcoming years.
- **It's user-friendly.** Users can access systems from a single dashboard, via browser or mobile app, all without using multiple credentials or additional systems like virtual private networks (VPNs).
- **It's future-proof.** Identity is a critical component in many innovations including Zero Trust, the Internet of Things (IoT), privacy, and freedom, and many others (learn more in Chapter 4). Your business can't get started on any of these initiatives without an IDaaS platform that evolves to address any uncertainty that may exist about the future.

The last word in Identity and Access Management

okta

okta.com

Move into the future of identity management

Identity and access management (IAM) solutions give your organization the ability to bolster security and manage identity and access with speed and confidence. To leverage identity services and security at scale, many organizations are adopting modern identity from the cloud — Identity as a Service (IDaaS). IDaaS provides robust and scalable IAM for an enterprise to secure and manage access for any user, from anywhere in the world on any device. In this book, you'll learn what modern identity is all about and how IDaaS can help your enterprise.

Inside…

- Tackle modern identity challenges
- Secure access with single sign-on (SSO) and multi-factor authentication (MFA)
- Automate account provisioning
- Secure cloud and on-prem apps, mobile and custom apps, servers, and APIs
- Address security and compliance
- Adopt a Zero Trust architecture

okta

Lawrence C. Miller has worked in information technology for more than 25 years and has written almost 200 For Dummies books. **Frederico Hakamine** is Technical Product Manager at Okta. He spends his time developing code and promoting the Okta Platform and APIs.

ISBN: 978-1-119-70867-4
Not For Resale

9 781119 708674

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT